IT PROJECT EVALUATION

Project Tracking No.: P-012-FY03-ITD

Return on Investment Program Funding Application (FY 2003 Request)

This is an electronic template. Please enter your responses on this document. Only electronic submittals of this template will be accepted. Proposals submitted after the designated due date may not receive funding consideration.
FINAL AUDIT REQUIRED: The Enterprise Quality Assurance Office of the Information Technology Department is required to perform a final project outcome audit, after implementation, for all Pooled Technology funded projects.

SECTION I: PROPOSAL

Date: 14 July 2001

Agency Name: Information Technology Department

Project Name: Information Security Program

Expenditure Name: Pooled Technology

Agency Manager: Kip Peters

Agency Manager Phone Number / E-mail: 5-0362/Kip.Peters@itd.state.ia.us

Executive Sponsor (Agency Director or Designee): Richard Varn

Request For ROI Application Waiver:

Agencies are required to complete this funding application when requesting funds for any project, any IT expenditure costing over $100,000, or any non-routine IT expenditure. If you feel there is compelling reason to waive this requirement, please provide (in the box provided below) a brief description of the project or expenditure, the budget amount, and a rationale for the waiver request. Until a decision is made regarding your waiver request, it is not necessary to complete any other portion of this application. The ITD Enterprise Quality Assurance Office will convey waiver request decisions within five working days of receipt.

Explanation: N/A

A. Project or Expenditure Rationale

Is this project or expenditure necessary for compliance with a Federal standard, initiative, or statute? ☐ **YES** (If "YES," explain) ☒ **NO**

Explanation: While the Information Security Program itself is not necessary for compliance with any known federal standards, initiatives, or statutes, the program has assisted agencies and the state in meeting federal security requirements, directives, and guidelines, and will continue to do so in the future. In particular, the program assists the Department of Revenue and Finance, Department of Human Services, and Information Technology Department with Internal Revenue Service (IRS) security audits while clarifying and helping these departments meet federal security requirements. Also, the program continues to assist the Department of Public Safety (DPS) meet requirements dictated by the Criminal Justice Information System Security Policy, published by the Federal Bureau of Investigation.

Is this project or expenditure required by State statute? ☐ **YES** (If "YES," explain) ☒ **NO**

Explanation: Iowa Code 14B stipulates that ITD develops security policy.

Does this project or expenditure meet a health, safety or security requirement?
☒ **YES** (If "YES," explain) ☐ **NO**

Explanation: Not only does the program help meet security requirements, it will be generating security requirements for the State of Iowa Enterprise. The program also contributes to the safety of state citizens by working with DPS in securing their networks and information, as well as by generating physical security requirements. It will also be assisting state entities in meeting Department of Health and Human Services security and privacy requirements as dictated by the Health Insurance Portability and Accountability Act (HIPAA), as well as developing the capability to conduct HIPAA assessments.

Is this project or expenditure necessary for compliance with an enterprise technology standard?
☒ **YES** (If "YES," explain) ☐ **NO**

Explanation: The program will be establishing enterprise technology standards; specifically, standards that deal with security of information and information systems.

Is this project or expenditure consistent with meeting the goals and objectives of the State's strategic plans?
☒ **YES** (If "YES," explain) ☐ **NO**

Explanation: The program is essential in meeting the State of Iowa's Digital Government and E-Commerce goals. Without effective security controls and practices in place, these goals will ultimately fail. In the absence of an enterprise program, individual programs will implement security independently and at differing levels of assurance; an enterprise program provides a cohesive security umbrella, ensuring that security efforts meet a consistent security policy, are adequate, and are cost-effective. Critical information will be available to authorized users when needed, and it will be protected from disclosure and unauthorized change. State agencies have many electronic plans and goals, including secure e-mail, secure web browser and server connections, virtual private networks, form signing, file encryption, and wireless applications; the security program will be a key enabler of achieving these goals. The success of the Governor's 100% E initiative depends in part upon this program.

Is this a "research and development" project or expenditure? ☐ **YES** (If "YES," explain) ☒ **NO**

Explanation:

B. Project or Expenditure Summary

1. Provide a pre-project or pre-expenditure (before implementation) and a post-project or post-expenditure (after implementation) description of the impacted system or process. In particular, note if the project or expenditure makes use of information technology in reengineering traditional government processes.

Response: The State of Iowa, in meeting its responsibilities to supply effective state services, plans to provide greater access and new services to state agencies, citizens, and business partners using new and existing state information systems. Sharing and making information available at the enterprise level presents both opportunities and challenges. The State of Iowa has the opportunity to become a leader in providing access to state information and services at the inter-agency and public levels. The challenge is to ensure that communications, information technology, tools, systems, and personnel provide a non-intrusive security environment while maintaining confidentiality, integrity, availability, and accountability of the information and information resources. This environment must provide reliable and secure information, in any required form, where and when needed.

In today's State of Iowa Enterprise, many systems are interconnected in some way. Because of this, security vulnerabilities in one system have an adverse effect on the security posture of other interfacing systems. Therefore, enterprise security is defined by the aggregate security posture of the State systems comprising the enterprise. The problem is, while many state agencies have a high degree of technical capability in controlling and protecting their information technology assets, this level of competence is not consistent throughout the enterprise, contributing to an unpredictable enterprise security posture.

The Information Security Program is designed to do several things. It will increase the level of consistency in agency security programs by developing and helping the agencies to conform to enterprise security policies, standards, and guidelines. It will also develop and implement a user security awareness training program, conduct network vulnerability assessments, establish and operate a risk management program, assist agencies with ad hoc security projects, plan, develop, and implement a State of Iowa Public Key Infrastructure (PKI), facilitate communication among the agencies concerning security vulnerabilities, incidents, and knowledge, develop security-related checklists and procedures, and identify, plan for, fund, and implement enterprise-level security technologies.

2. Summarize the extent to which the project or expenditure improves customer service to Iowa citizens or within State government. Included would be such items as improving the quality of life, reducing the government hassle factor, providing enhanced services, improving work processes, etc.

Response: The result of these security initiatives will be an enterprise with enhanced security and appropriate access to the systems that make up the enterprise, thereby benefiting the agencies, their partners, and their customers. Important information will be available to authorized users while also being protected from disclosure and unauthorized alteration. This is important not only to state government, but also to its citizens and business partners. Through the 100% E initiative, the state will provide enhanced service to its citizens and other digital initiatives, such as JetForms, will improve current work processes. Security will be in important part of the implementation of these programs.

3. Identify the main project or expenditure stakeholders and summarize the extent to which each, especially citizens, is impacted. In particular, note if the project or expenditure helps reconnect Iowans to State government.

Response: A program of this magnitude has many stakeholders; it is not unreasonable to identify all state citizens, agencies, and business partners as stakeholders that will be impacted by the project. All present Iowa citizens, and many past citizens, have personal information that is stored, processed, and/or disseminated by state government computer systems. They all have a stake in the protection of that information. All agencies, even non-participating agencies, will benefit by the increased security of the enterprise, since most of these agencies either share some of the same architecture or have information that is stored on Iowa mainframes or other agency systems. In today's interconnected world, if a vulnerability leads to a compromise in one system, it may lead to unintended privileged access to information on other systems. If business partners are to conduct business electronically with the state, it is important that their interests are protected as well.

SECTION II: PROJECT ADMINISTRATION

A. Agency Information

1. Project Executive Sponsor Responsibilities: The sponsor must have the authority to ensure that adequate resources are available for the entire project, that there is commitment and support for the project, and that the organization will achieve successful project implementation.

Response: No response required.

2. Organization Skills:
   a. List the project management skills necessary for successful project implementation
   b. List the project management skills available within the agency
   c. List the source(s) of project management skills lacking within the agency
   d. Summarize relevant agency project management experience and results

Response:
a. Project management skills necessary for successful implementation include: planning, budgeting, coordinating, communicating, managing, and leading.
b. These skills are all currently available within the program.
c. N/A
d. The Chief Information Security Officer has extensive project and program management experience at the multi-million dollar level. This includes projects and programs in support of multi-billion dollar programs.

B. Project Information

1. History:
   a. Is this project the first part of a future, larger project? If so, please explain.
   b. Is this project a continuation of a previously begun project? If so, please explain project history, current status, and results.

Response: The security program is an integral part of ITD operations and is essential to the successful implementation of Digital Government. It is a continuation of a previous project and is continuing to build its capabilities. A capability to provide vulnerability assessments has been developed, and agency assessments are on-going, saving the state over $300,000 per year. Personnel and programs are in place to provide near real-time intrusion detection and incident response, as well as notification of serious vulnerabilities. A test lab has been installed, allowing valuable security testing to be conducted when needed. Security consulting services have been made available for all agencies, either participating or not. Much time has been spent working with ITD on its internal security and the security of the digital government/e-commerce environment. The majority of the basics of the program have been put in place; it is now poised to move into providing a higher level of assurance with its initiatives, programs, and capabilities.

2. Expectations: Describe the primary purpose or reason for the project.

Response: The Information Security Program is designed to do several things. It will increase the level of consistency in agency security programs by developing and helping the agencies to conform to enterprise security policies, standards, and guidelines. It will also develop and implement a user security awareness training program, conduct network vulnerability assessments, establish and operate a risk management program, assist agencies with ad hoc security projects, plan, develop, and implement a State of Iowa Public Key Infrastructure (PKI), facilitate communication among the agencies concerning security vulnerabilities, incidents, and knowledge, develop security-related checklists and procedures, as well as identify, plan for, fund, and implement enterprise-level security technologies.

The result will be an enterprise with enhanced security and appropriate access to all the systems that make up the enterprise, thereby benefiting the agencies, their partners, and their customers. Important information will be available to authorized users, while also being protected from disclosure and unauthorized change. This is important not only to state government, but also to its citizens and business partners.

The ultimate goal of the information security program is to ensure the availability, integrity, and confidentiality of enterprise information and information technology resources by implementing a statewide enterprise security program that is uniformly implemented and consistently enforced throughout each state entity (agency, commission, authority, etc.). This will be done with the concept of information assurance in mind: protecting the information and information systems; detecting incidents as they occur; restoring sytems as necessary; and responding appropriately to the event. Other goals include:

· Identifying opportunities for agencies to collaborate on security technology purchases, maintenance, and training, saving money through economies of scale while increasing security.
· Protecting the State of Iowa from liabilities and embarrassment associated with the loss/damage/exposure of sensitive and confidential data.
· Promoting the exchange of information among State of Iowa organizations to facilitate the development of knowledge and understanding regarding information security.

Program objectives, as identified in the program's risk management plan, are to:

1. Provide appropriate levels of confidentiality, integrity, availability, and assurance for Iowa information systems and the information that Iowa processes.
    a. Satisfy e-government objectives in a secure manner.
    b. Raise the security awareness of all users of Iowa IT to an appropriate level.
    c. Maintain trust level of stakeholders that supply data.
    d. Establish and maintain an effective security risk management program.
        i. Identify data that needs to be safeguarded.
        ii. Establish guidelines for classification levels.
    e. Enforce privacy as defined by state and federal laws, policy and regulations.
    f. Define a set of Policies and Standards for security that will be applied to participating (as defined in ITD legislation) Iowa IT systems.
    g. Detect unauthorized activity and respond appropriately.
    h. Assess damage and recover applicable systems and data after an incident occurs.
    i. Investigate incidents and make necessary changes.
2. Have a minimum impact on established security safeguards in existing programs.
3. Minimize impact on user ability to access appropriate information.
4. Develop and maintain stakeholder input to the program.
5. Collaborate with appropriate stakeholder agencies in the development, implementation and maintenance of the program.
6. Establish a security program/presence in each agency - includes POC within each agency
7. Identify techniques/methods to aid agencies with inadequate security related resources· Develop, implement, and monitor the Information Security Program.

3. Measures: Describe the criteria that will be used to determine if the project is successful.

Response: It is difficult to ascertain the successful nature of a security program. Most security programs are deemed successful if nothing happens; that is, no major incident occurs, or a minimum number of incidents occur and are recovered from in a timely and cost effective manner. However, that is not a truly accurate assessment, as a company, state government, or other entity can escape incident just by being lucky. The information security program can be determined successful if the following items become reality:

· Security problems are identified, prioritized, and fixed.
· Users are educated on security issues and awareness.
· Consistent security policies are developed, implemented, and enforced (at both the enterprise and agency levels).
· Security is considered throughout the system life cycle.
· Security standards are developed and promulgated.
· Communication among State security professionals is enhanced.

If the project fails, then the situation remains what it is today; at best, multiple ad-hoc security programs implementing security with differing levels of assurance.

4. Environment: List the project participants (i.e. single agency, multiple agencies, State government enterprise, citizens, associations, or businesses, etc.).

Response: The entire State government enterprise as well as necessary and appropriate private and other public sector organizations will be actively involved in the continuing implementation of the Information Security Program. The program will depend upon the input and participation of the agencies; they will be developing their own policies, implementing their own procedures, and securing their own systems under the guidance of the program. The program is not intended to actively (i.e., hands-on) secure every agency and every system; it is intended to provide a higher level of guidance, coordination, and communication. All agencies will provide input based upon their current business processes and user interaction.

5. Risk: Describe the project risks which may be internal or external to State government, i.e. implementing versus not implementing project, changing technology, potential cost overruns, changing citizen demand or need, etc.

Response: The security program has developed a program risk management plan, in conjunction with many of the stakeholders, in an effort to manage the risk associated with the program. This plan describes the standardized, structured process the Information Security Program uses to identify, categorize, analyze, and mitigate risks associated with the program. This plan also describes the method used to determine risk status and measure the progress of risk mitigation efforts. The risk management approach documented in this plan is based on proven risk management techniques developed by the Software Productivity Consortium. The plan is attached to this document, in addition to the program's risk spreadsheet and risk table which identify the risks associated with the program.

6. Security / Data Integrity / Data Accuracy / Information Privacy
   a. List the security requirements of the project
   b. Describe how the security requirements will be integrated into the project and tested
   c. Describe what measures will be taken to insure data integrity, data accuracy and information privacy.

Response: State of Iowa security vulnerability and risk information is critical information and will be protected as such by a combination of technical and procedural security controls.

7. Project Schedule
   Describe general time lines, resources, tasks, checkpoints, deliverables, responsible parties, etc.

Response:

- Security Vulnerability Assessments	Ongoing
- Intrusion Monitoring	Ongoing
- Other Daily Security Activities	Ongoing
- Enterprise Security Policy	September 2001
- Risk Management Program Phase I	10/2001 - 10/2002
- Risk Management Program Phase II	10/2002 - 10/2003

SECTION III: TECHNOLOGY (In written detail, describe the following)

A. Current Technology Environment

1. Software (Client Side / Server Side / Midrange / Mainframe):
   a. Application software
   b. Operating system software
   c. Major interfaces to other systems, both internal and external

Response: This project does not lend itself to readily identify the hardware and software of the current and proposed environment. This is due to three reasons. First, the program is intended to address the entire State of Iowa Enterprise comprised of many interfacing client, server, midrange, and mainframe systems. This includes all systems of all types of hardware and software, many of which are unknown at this time, in many different logical and physical environments, interfacing with both internal and external systems. Second, the program by its very nature has some unknown elements at this point. The risk management program itself must continue to be developed and implemented in order to determine what security features are lacking; once the deficits are identified the needs will have to be prioritized and implemented as funding permits. Third, the program isn't 100% hardware and software oriented. Much of the security program involves policy, procedures, guidelines, communication, education, and awareness.

2. Hardware (Client Side / Server Side / Mid-range / Mainframe):
   a. Platform, operating system
   b. Storage and physical environment
   c. Connectivity and bandwidth
   d. Logical and physical connectivity
   e. Major interfaces to other systems, both internal and external

Response: See previous response.

B. Proposed Technology Environment

1. Software (Client Side / Server side / Mid-range / Mainframe)
   a. Application software
   b. Operating system software
   c. Major interfaces to other systems, both internal and external
   d. General parameters if specific parameters are unknown or to be determined

Response: See previous response.

2. Hardware (Client Side / Server Side / Mid-range / Mainframe)
   a. Platform, operating system
   b. Storage and physical environment
   c. Connectivity and Bandwidth
   d. Logical and physical connectivity
   e. Major interfaces to other systems, both internal and external
   f. General parameters if specific parameters are unknown or to be determined

Response: See previous response.

C. Data Elements

If the project creates a new database, provide a description of the data elements.

Response: N/A

SECTION IV: Financial Analysis

A. Budget: Enter figures and calculate (see formula below) Total Annual Prorated Cost (State Share).

$$\left[\left(\frac{Budget\ Amount}{Useful\ Life}\right)\times \%\ State\ Share\right]+\left(Annual\ Ongoing\ Cost\times \%\ State\ Share\right)=Annual\ \Pr orated\ Cost$$

Budget Line Items	Budget Amount (1st Year Cost)	Useful Life (Years)	% State Share	Annual Ongoing Cost (After 1st Year)	% State Share	Annual Prorated Cost
Agency Staff	$600000	1	100%	$625000	100%	$1225000
Software	$5000	4	100%	$1000	100%	$2250
Hardware	$10000	3	100%	$10000	100%	$13333
Training	$10000	1	100%	$10000	100%	$20000
Facilities	$	1	%	$	%	$
Professional Services	$	4	%	$	%	$
ITD Services	$	4	%	$	%	$
Supplies, Maint, etc.	$5000	1	100%	$5000	100%	$10000
Other (Specify)	$	1	%	$	%	$
Totals	$630000	-------	-------	$651000	------	$1270583

Transfer this amount to the ROI Financial Worksheet, item “D” on page 16.

B. Funding: Enter data or provide response as requested

1. This is (pick one):
   - ☒ A Pooled Technology Fund or Reengineering Fund Request
   - ☐ An Agency IT Expenditure or Budget Request (General Fund, Road Funds, etc)
   - ☐ Other – Specify:

2. On a fiscal year basis, enter the estimated cost by funding source?

	FY03		FY04		FY05	
	Cost ($)	% Total Cost	Cost ($)	% Total Cost	Cost ($)	% Total Cost
State General Fund	$	%	$	%	$	%
Pooled Tech. Fund	$630000	100%	$650000	100%	$700000	100%
Federal Funds	$	%	$	%	$	%
Local Gov. Funds	$	%	$	%	$	%
Grant or Private Funds	$	%	$	%	$	%
Other Funds (Specify)	$	%	$	%	$	%
Total Project Cost	$630000	100%	$650000	100%	$700000	100%

If applicable, summarize prior fiscal year funding experience for the project / expenditure.

Response: For FY01, the security program had a budget of $1.1 million.

1. On a fiscal year basis, how much of the total ($ amount and %) project / expenditure cost would be absorbed by your agency from normal operating budgets (all funding sources)?

Response: 0%

2. Identify, list, and quantify all new annual ongoing (maintenance, staffing, etc.) related costs (State $s) that will be incurred after implementation or expenditure.

Response:
- Hardware/software maintenance: $14,000
- Staffing: $625,000
- Training: $10,000
- Misc. $5,000

C. ROI Financial Worksheet: Respond to the following and transfer data to the ROI Financial Worksheet (see IVC11) as necessary:

1. Annual Pre-Project Cost – Quantify all actual state government direct and indirect costs (personnel, support, equipment, etc.) associated with the activity, system or process prior to project implementation. This section should be completed only if state government operations costs are expected to be reduced as a result of project implementation.

Response: N/A

2. Annual Post-Project Cost – Quantify all estimated State government direct and indirect costs associated with activity, system or process after project implementation. This section should be completed only if State government operations costs are expected to be reduced as a result of project implementation.

Response: N/A

3. State Government Benefit -- Subtract the total "Annual Post-Project Cost" from the total "Annual Pre-Project Cost." This section should be completed only if State government operations costs are expected to be reduced as a result of project implementation.

Response: N/A

4. Citizen Benefit – Quantify the estimated annual value of the project to Iowa citizens**.** This includes the "hard cost" value of avoiding expenses ("hidden taxes") related to conducting business with State government. These expenses may be of a personal or business nature. They could be related to transportation, the time expended on or waiting for the manual processing of governmental paperwork such as licenses or applications, taking time off work, mailing, or other similar expenses. As a "rule of thumb," use a value of $10 per hour for citizen time savings and $.325 per mile for travel cost savings.

Response: The number of possible incidents that could be presented is practically endless. Due to that fact, the estimated potential costs associated with two levels of security incidents are detailed below:

Event 1 (Minor): Natural Resources E-mail server being used as SPAM relay

- Governmental costs to recover from the incident: $5000.00
- Indirect costs due to lost productivity: $25,000.00
- Potential revenue loss to State of Iowa due to Natural Resources employees being unavailable via e-mail to potential customers and other parties, as well as possible litigation due to an Iowa State government system being used to harass individuals and businesses: $1,000,000.00+

Event 2 (Major): A critical system is compromised that contains citizen personal and credit card information. This information is posted on the Internet and many instances occur where the information is used to purchase items using those particular credit card numbers. In other cases, identities are assumed with associated damages that include purchases of everything from cars to homes and property. (This is not made up - both of these scenarios have occurred, although not to Iowa government systems. The FBI reports that identity theft is one of the fastest growing crimes in the nation. They also indicate that if somebody is the victim of identity theft, it most likely will affect them in some way the rest of their lives. Some incidents of identity theft involve selling the identities to illegal immigrants.)

- Governmental costs, associated with that one system, to recover from the incident: $75,000.00
- Governmental costs to identify and notify citizens who had their information posted: $100,000.00
- Governmental costs to determine integrity of other systems' information: $500,000.00
- Governmental liability due to lawsuits from the banks that issued the credit cards: $5,000,000.00
- Governmental liability due to lawsuits from other affected parties, such as mortgage companies: $10,000,000.00
- Governmental liability due to citizen lawsuits: $20,000,000.00
- Total governmental liability: $35,675,000.00

- Citizen costs to cancel cards, obtain new cards, and restore credit record: $1,000.00 each
- Citizen costs incurred due to reducted credit rating: $2,000.00 each
- Total Citizen Cost for loss of services: $3,000.00 each

Estimated 50 citizens / year $3,000.00 X 50 = $150,000.00

- Other costs incurred by citizens that are not necessarily monetary in nature include the following:
  - Time spent to cancel credit cards.
  - Time spent to deal with new, unknown bills that arrive.
  - Time spent notifying and dealing with applicable authorities: employer personnel department, IRS, FBI, Social Security, banks, credit unions, credit bureaus, credit card companies, and local law enforcement entities.
  - Dealing with the issue for the foreseeable future.
  - Dealing with the possibility of being denied future credit.
  - Having to possibly change their identity.
- Governmental damage due to the loss of citizen trust: $Unknown

Although the second event may seem farfetched, it has happened and it will happen again. Will it happen because of an Iowa governmental system? Nobody can predict that, but it is certain that events of some nature will occur. They have occurred. The enormity of any event is difficult to predict, but you must have the due diligence to properly prepare.

As the State moves ahead with its digital government and e-commerce initiatives, it will open itself up to further risk; therefore, it is imperative to properly secure the systems. As custodians of citizen information and money, we should be incredibly worried about the possibilities.

5. Opportunity Value/Risk or Loss Avoidance Benefit – Quantify the estimated annual non-operations benefit to State government. This could include such items as qualifying for additional matching funds, avoiding the loss of matching funds, avoiding program penalties/sanctions or interest charges, avoiding risks to health/security/safety, avoiding the consequences of not complying with State or federal laws, providing enhanced services, avoiding the consequences of not complying with enterprise technology standards, etc.

Response:
- Anticipated HIPAA funds: $100,000
- Federal sanctions issued for inadequate security measures: $2,000,000

6. Total Annual Project Benefit -- Add the values of all annual benefit categories.

Response: $37,100,000

7. Total Annual Project Cost – It is necessary to estimate and assign a useful life figure to each cost identified in the project budget. Useful life is the amount of time that project related equipment, products, or services are utilized before they are updated or replaced. In general, the useful life of hardware is three (3) years and the useful life of software is four (4) years. Depending upon the nature of the expense, the useful life for other project costs will vary between one (1) and four (4) years. On an exception basis, the useful life of individual project elements or the project as a whole may exceed four (4) years. Additionally, the ROI calculation must include all new annual ongoing costs that are project related. Completing Section IV-A, Project Budget of the evaluation document will provide all the necessary information for this item.

Response: See Section IV-A.

8. Benefit / Cost Ratio – Divide the "Total Annual Project Benefit" by the "Total Annual Project Cost." If the resulting figure is greater than one (1.00), then the annual project benefits exceed the annual project cost. If the resulting figure is less than one (1.00), then the annual project benefits are less than the annual project cost.

Response: 33

9. ROI -- Subtract the "Total Annual Project Cost" from the "Total Annual Project Benefit" and divide by the amount of the requested State IT project funds.

Response: 58

10. Benefits Not Readily Quantifiable -- List the project benefits which are not readily quantifiable (i.e. IT innovation, unique system application, utilization of new technology, hidden taxes, improving the quality of life, reducing the government hassle factor, meeting a strategic goal, etc.). Rate the importance of these benefits on a "1 – 10" basis, with "10" being of highest importance. Check the "Benefits Not Readily Quantifiable" box in the applicable row.

Response: Due to the nature of the project for which funding is being sought, the calculation of a return on investment is difficult to perform with certainty. The implementation of the Information Security Program will not necessarily lead to monetary savings. In fact, some costs in some agencies could increase slightly. This could be due to additional monitoring that must take place or additional equipment required to further secure certain IT systems. Other agencies may decrease costs as individual security programs are streamlined, consolidated, and implemented in a more cost-effective manner.

The difficulty of determining a monetary benefit arises because the main goal of the security program is to try to stop bad things from happening. Money is spent to protect information and information systems, and if done well, events will not happen very frequently, and those that do occur will be recovered from quickly, appropriately, and cost-effectively. The nature of the program is such that if implemented with a high level of assurance, the data required to determine a return on investment will not exist. In the absence of this data, a specific return on investment is hard to establish; therefore, historical information from other venues must be used as evidence as to the beneficial nature of the program in monetary terms.

There are significant benefits to be realized by implementing this program. Having consistent, specific security policies (rating = 10) will ensure that all agencies have the appropriate level of oversight on information security. Assessing system security and putting appropriate technical and procedural measures in place (9) to close security gaps will help ensure that intentional and unintentional breaches do not occur. Published averages vary considerably, but one thing is certain: the monetary costs associated with security incidents are substantial. These costs may include those associated with system rebuild, damage assessment, data recovery, system unavailability, civil lawsuit, and data integrity verification.

The non-monetary costs of potential breaches range anywhere from embarrassment (5) to loss of life (10). These costs are significant as well and will be minimized by implementing an enterprise information security solution.

Other benefits include the following items:

· State government will fulfill its statutory requirements with regard to data privacy and data integrity concerns (10).
· This project will raise and maintain awareness of computer security with individual agencies and will provide an enterprise direction for individual agency security programs (8).
· Citizens of Iowa will have an increased confidence in their government's ability to secure confidential data from accidental release (10).
· Money will no longer be wasted on inadequate, inferior, and/or non-standard security solutions (8).
· The State of Iowa will be able to pursue initiatives of providing greater access to information and services to employees and citizens while protecting sensitive information (9).
· The State of Iowa will be better able to obtain its Digital Government and E-Commerce goals (9).
· State citizens, businesses, and employees will have access to information and will be able to conduct business on-line, reducing the frustrations often evident in doing business with the state government bureaucracy (8).

11. ROI Financial Worksheet

Annual Pre-Project Cost - How You Perform The Function(s) Now	
FTE Cost (salary plus benefits):	$0
Support Cost (i.e. office supplies, telephone, pagers, travel, etc.):	$0
Other Cost (expense items other than FTEs & support costs, i.e. indirect costs if applicable, etc.):	$0
A. Total Annual Pre-Project Cost:	$0
Annual Post-Project Cost – How You Propose to Perform the Function(s)	
FTE Cost:	$0
Support Cost (i.e. office supplies, telephone, pagers, travel, etc.):	$0
Other Cost (expense items other than FTEs & support costs, i.e. indirect costs if applicable, etc.):	$0
B. Total Annual Post-Project Cost:	$0
State Government Benefit (= A-B):	$0
Annual Benefit Summary	
State Government Benefit:	$0
Citizen Benefit:	$35000000
Opportunity Value or Risk/Loss Avoidance Benefit:	$2100000
C. Total Annual Project Benefit:	$37100000
D. Annual Prorated Cost (SECTION IV-A):	$1270583
Benefit / Cost Ratio: (C / D) =	29
Return On Investment (ROI): (C – D / Requested Project Funds) x 100 =	5687**%**
☐ **Benefits Not Readily Quantifiable**	

Section V: ITC Project Evaluation Criteria

Criteria and Location in Project Evaluation Document		Points
1.	Is the project a statutory requirement; legal requirement; federal or state mandate; health, safety or security requirement or issue; and/or required for compliance with the enterprise technology standards? **Location: Section I-A**	**15**
2.	Will the project improve customer service? **Location: Section I-B.2**	**15**
3.	Does the project have a direct impact on citizens? To what extent does the project help reconnect state government with Iowans? **Location: Section I-B.3**	**10**
4.	Does the project provide a sufficient tangible and/or intangible return on investment? Will it generate savings or income? **Location: Section IV-C**	**10**
5.	Does the project make use of information technology and its practical application in reengineering traditional government processes consistent with the goals and objectives of the state's strategic plans? **Location: Section I-B.1**	**10**
6.	Risk: What are the risks associated with the project? Such risks may include those internal and external to state government, the risk of doing a project, the risk of not doing a project, and the risks associated with changing technologies, potential cost overruns, and changing citizen demands and needs. **Location: Section II-B.5**	**10**
7.	Is this funding required to continue a project that was begun prior to the year funding is being requested for and does it have proven past performance? Is the funding part of a multi-year strategy? **Location: Section II-B1, IVB2**	**10**
8.	Will the project be for only one agency, multiple agencies, or the state government enterprise? **Location: Section I-B3, IIB4**	**10**
9.	Has the applicant maximized their own and other resources in the project? Is alternative funding unavailable for this project? (If no other funding available, project will not be completed without Pooled Technology funding) **Location: Section IV-B.2, IV-B.3**	**5**
10.	What is the credibility of the requester based on past performance on other projects? **Location: Section II-A.2.d**	**5**
	Total	**100**